REMARKS

The Examiner has objected to the application title. The Examiner has rejected claims 10-14 under 35 USC 112. The Examiner has rejected claim 15 as being anticipated by U.S. Patent Application Publication 2002/0095569 to Jerdonek ("Jerdonek"). The Examiner has rejected claims 1-14 and 16-18 as being obvious over Jerdonek in combination with various combinations of *Cryptography and Network Security* by William Stallings ("Stallings"); U.S. Patent Number 6,075,860 to Ketcham ("Ketcham"); U.S. Patent Application Publication 2003/0037250 in the name of Walker et al. ("Walker") and U.S. Patent Application Publication 2002/0101857 in the name of Heller ("Heller").

Objection to the Specification:

Applicant has amended the title according to the Examiner's suggestion. Applicant respectfully submits that this amendment fully addresses the Examiner's objection to the specification.

Rejections under 35 USC 112:

Applicant has amended claim 10 to remove the ambiguity identified by the Examiner. Applicant respectfully submits that this amendment fully addresses the Examiner's rejections under 35 USC 112 and withdrawal of same is respectfully requested.

Rejections under 35 USC 102:

The Examiner has rejected claim 15 under 35 USC 102 as being anticipated by U.S. Patent Application Publication 2002/0095569 to Jerdonek ("Jerdonek"). In support of this rejection, the Examiner has asserted the following:

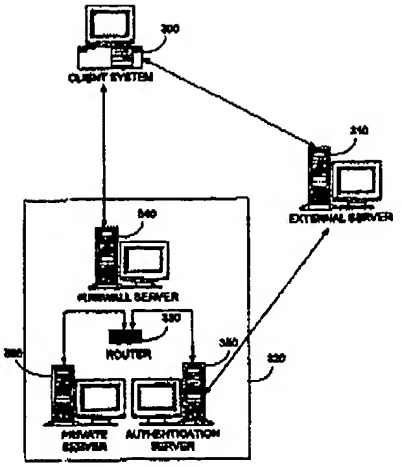
> As per independent claim 15, '569 teaches a client device ('key wallet' paragraphs 39-40) installed I a data network access device (client systems, Figure 1, systems 130, 140, 150). ... Means for requesting access to the remote data network utilizing the preprogrammed common key set for authentication purposes when the client device is installed in the network access device is taught in paragraph 44. Means for receiving a new user key set from the network is taught in paragraphs 47-48. These paragraphs along with paragraphs 49-53 indicate that the common key set is replaced with the new key set, as the new key set is used to connect to the remote server. Means responsive to receiving the new user key set for automatically requesting access to the remote data network utilizing the new user key set for authentication purposes is also taught in paragraphs 47-48, and paragraph 61 teaches that it may be automatic.

As set out in detail below, Applicant respectfully submits that Jerdonek does not anticipate claim 15, as amended.

The Jerdonek reference

Jerdonek discloses a client computing system including a processor that requests a challenge from an authentication server and receives the challenge from the authentication server via a first secure communications channel. The processor receives user authentication data from a user and determines a private key and a digital certificate in response to the user authentication data. The processor forms a digital signature in response to the identity code and the private key, communicates the digital signature to the

authentication server, communicates the digital certificate to the authentication server and communicates network user authentication data and the identity code to the authentication server via a security server. The authentication server activates the identity code when the digital signature is verified.



Applicant respectfully submits that the Examiner's rejection of claim 15 as being anticipated by Jerdonek is improper. It is clear from the office action that the Examiner is reading the "means-plus-function" in its broadest possible generic sense, and not in the specific sense explicitly required by the patent laws. Under the law, a "means-plus-function" limitation is not properly interpreted as any conceivable means for performing the recited function. The means recited in the claim is limited to the corresponding means disclosed in the specification for performing the recited function.

Nevertheless, solely in order to expedite prosecution of the present application, Applicant has amended claim 15 in order to recite a "means for conducting a registration session with a registration server." Accordingly, Applicant respectfully submits that claim 15 is even more clearly distinguishable over the Jerdonek reference, and the Examiner is respectfully rquested to withdraw the rejection of claim 15 as being anticipated by Jerdonek.

Rejections under 35 USC 103:

The Examiner has rejected claims 1-8 and 10 as being obvious over Jerdonek in view of Stallings. Claim 1 reads as follows:

> 1. A method of automatically configuring and authenticating a client device installed in a data network access device at a user's premises, said network access device including an Internet Protocol (IP) router that routes IP signaling between a remote data network and a plurality of users connected to the network access device at the premises, said method comprising the steps of:
>
> preprogramming the client device with a common key set;
>
> requesting access to the remote data network by the client device using the preprogrammed common key set for authentication purposes;
>
> ***determining by an authenticator in the network*** whether the common key set is valid;
>
> providing the client device with limited network access, said limited access enabling the client device to access only a registration server, upon determining that the common key set is valid;
>
> ***accessing the registration server;***
>
> sending a new user key set to the client device;
>
> automatically requesting access to the remote data network by the client device using the new user key set for authentication purposes;
>
> ***determining by the authenticator*** whether the new user key set is valid; and
>
> providing the client device with full network access, upon determining that the new user key set is valid.

The Examiner has conceded that Jedonek does not anticipate any of claims 1-14 and 16-18. Specifically, the Examiner has conceded that Jerdonek does not teach an authenticator programmed to determine whether both the common key set and the new user key set are valid. The Examiner asserts that authentication of a common key and a new user key by a single authenticator are taught by Stallings, and that it would be obvious to combine Jerdonek with

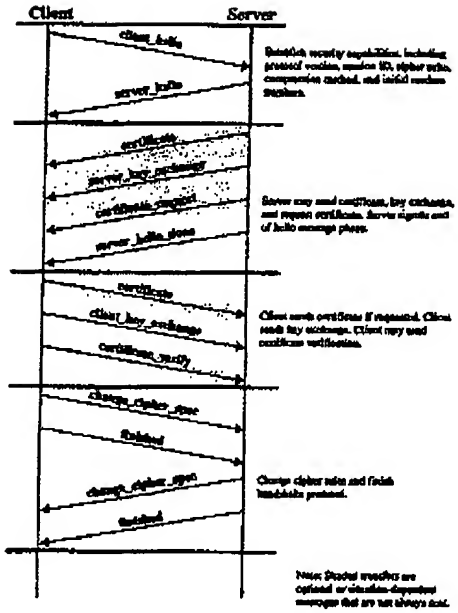
Stallings in order to derive the subject matter of independent claims 1 and 10.

As noted above, the Examiner himself has conceded that Jerdonek fails to teach that the "external server 310" authenticates both the common key set and the new user key set. Applicant respectfully submits that Jerdonek additionally fails to teach other limitations recited within the pending claims, including but not limited to the three-step, two server authentication process recited in claims 1 and 10. Further, Jerdonek teaches that the "external server," which the Examiner is equating to the "authenticator" recited in the claims, is external to the network, and not *within the network* as explicitly recited in claims 1 and 10. The Examiner cites Stallings in order to overcome the numerous deficiencies of Jerdonek. As discussed in further detail below, Stallings does not overcome these numerous deficiencies of Jerdonek.

The Stallings reference

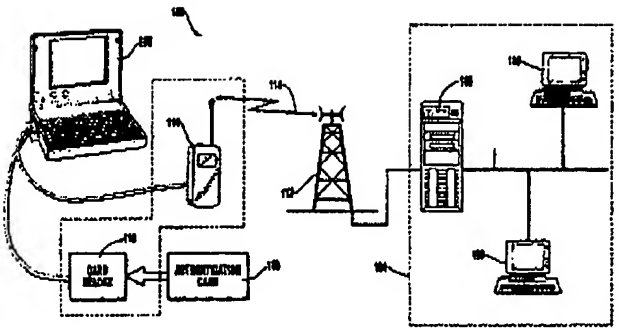
Stallings discloses a secure handshaking protocol employed between a single client and a single server. The Examiner has cited Stallings for a teaching of SSL handshaking. Although Applicant agrees that Stallings generally discloses an SSL handshaking protocol, Stallings does not appear to cure the deficiencies of Jerdonek as regards the pending claims. Stallings does not, for example, disclose a "common key set" and a "new user key set," or separate authentication and registration servers as

recited in the pending claims. Stallings does not disclose the granting of multiple levels of access to a remote data network depending on a multiple stage authentication process involving multiple servers. Stallings does not disclose that the authentication server is *within the network*, as recited in claims 1 and 10.



The Examiner has failed to point out how and in what manner Stallings supposedly teaches the combination of limitations conceded to be missing from Jerdonek. In addition to the limitations recited above, it appears that Stallings further fails to teach additional limitations, including the step of providing the client system with limited network access after authentication of the common key set. Accordingly, Applicant respectfully submits that the Examiner's assertion that Stallings cures the deficiencies of Jerdonek is not supported by the teachings of the reference, and Applicant respectfully submits that the Examiner has failed to establish a prima facie case of obviousness of claims 1-8 and 10.

The Ketcham reference



The Examiner has rejected claims 9, 12 and 16-18 as being obvious over Jerdonek, Stallings and Ketcham. Ketcham discloses a method and system for authenticating an authorized user of a remote terminal attempting to interconnect with a computer network over a wireless modem. An encrypted wireless communication channel is established between a remote terminal and a network server for facilitating the authentication process. An authorized user presents an authentication card containing credentials including a user identifier and an authentication encryption key to a remote terminal. The remote terminal establishes a wireless communication channel with a network server which provides a firewall between unauthenticated users and a computer network. The network server and the remote terminal then exchange encrypted information thus verifying the authenticity of each party. The remote terminal and the network server each independently generate a data encryption key for use in establishing a secure encrypted wireless communication channel therebetween. The Examiner has cited Ketcham for a teaching of "authenticating by the client device that the new user key set is received from a valid source." The Examiner has not asserted that Ketcham cures the deficiencies of Jerdonek and Stallings as regards independent claims 1, 10 and 15, and Applicant

respectfully submits that Ketcham fails to do so. Accordingly, Applicant respectfully submits that claims 9, 12 and 16-18 are allowable for the same reasons as claims 1, 10 and 15 from which they depend.

The Walker reference

The Examiner has rejected claim 11 as being obvious over the combination of Jerdonek, Stallings and Walker. Walker discloses a secured access controller for use in connection with a network that communicates with content servers that store content objects and client processing systems that request access to the stored content objects. The secured access controller comprises: 1) a database for storing a plurality of encryption keys and a plurality of decoding keys associated with selected ones of the content servers and the client processing systems; and 2) an encryption controller for receiving from a first one of the client processing systems an access request for a first selected one of the content objects stored on a first one of the content servers and, in response thereto, generating a first encryption key and transmitting the first encryption key to the first client processing system, wherein the first encryption key is usable by the first client processing system to encrypt client messages transmitted to the secured access controller. The Examiner has cited Walker for a teaching of "an authentication database that associates a plurality of common key sets with a plurality of registration servers." The Examiner has not asserted that Walker cures the above-recited deficiencies of

Jerdonek and Stallings as regards the pending independent claims. Accordingly, Applicant respectfully submits that claim 11 is allowable for the same reason as claim 10 from which it depends.

The Heller reference

The Examiner has rejected claims 13-14 and 17-18 as being obvious over the combination of Jerdonek, Stallings and Heller. Heller discloses a method and system for transmitting information from a computer to a server utilizing point-to-point protocol (PPP) in a mobile environment. The system enables a PPP session to be maintained between a user device and a PPP termination device while the user device is mobile. A mobile IP address is assigned to customer premise equipment (CPE) device associated with a user device, e.g., a PC. The CPE includes a Mobile IP Mobile Node and L2TP access concentrator (LAC) functionality. The Mobile IP address is then registered with a Mobile IP Home Agent associated with the home network for the assigned Mobile IP address. The PC initiates a point-to-point protocol (PPP) session to the LAC within the CPE. The LAC initiates an L2TP session to an LNS. The Examiner has cited Heller for a teaching of "the client device utilizes the Point-to-Point Protocol (PPP) for signaling with the authenticator and registration server" and "the client device is installed in a Customer Premises Equipment (CPE) comprising a Digital Subscriber Line (DSL) modem and IP router." The Examiner has not asserted that Walker cures the above-recited deficiencies of Jerdonek and Stallings as regards the pending independent claims, and Applicatnt

respectfully submits that Walker does not do so. Accordingly, Applicant respectfully submits that claims 13-14 and 17-18 are allowable for the same reasons as independent claims 10 and 15 from which they depend.

Fee Statement

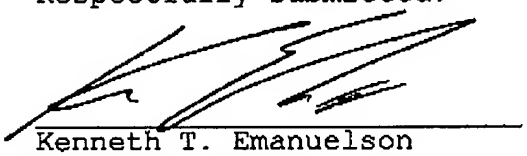
The number of independent claims has remained the same and the total number of claims has remained the same. Applicant believes no fees are due in conjunction with the filing of this Response. If fees are due, however, please debit our deposit account, Account No. 03-1130.

CONCLUSION

Applicants have explained, with specificity, that none of the cited references anticipates any of the pending claims and that the proposed combinations of the cited references do not render any of the pending claims obvious. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 1-18 under 35 U.S.C. 112, 35 U.S.C. 102 and 35 U.S.C. 103(a) and issue a Notice of Allowance of pending claims 1-18. The Examiner is encouraged to call the undersigned for any reason which may advance the present case to issuance.

Dated this 1st day of June, 2006.

Respectfully submitted:



Kenneth T. Emanuelson
Reg. No. 46,684
Danamraj & Youst, P.C.
Premier Place, Suite 1450
5910 North Central Expressway
Dallas, Texas 75206
Tel 214-750-5666
Fax 214-363-8177